

Verkettung von Profilen als Risiko bei der Auftragsverarbeitung

Tilmann Fleck / Johannes Nehlsen

Julius-Maximilians-Universität Würzburg

Stabsstelle

Herbstakademie 2025

Informationen zu den Referenten / Autoren

Johannes Nehlsen, Regierungsrat

Leiter der Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen

Nebentätigkeit:

Datenschutzberatung über die actago GmbH

Mail: johannes.nehlsen@uni-wuerzburg.de



Tilmann Fleck

Studentische Hilfskraft der Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen

Mail: gustav.fleck@uni-wuerzburg.de



Agenda

1. Ausgangslage & Problemstellung
2. Profilverkettung – Was ist das?
3. Mögliche zulässige Mit- und Eigennutzungen
4. Risiken für Betroffene und Auswirkungen
5. Lösungsansätze – Vertraglich
6. Technisch-organisatorische Maßnahmen
7. Fazit

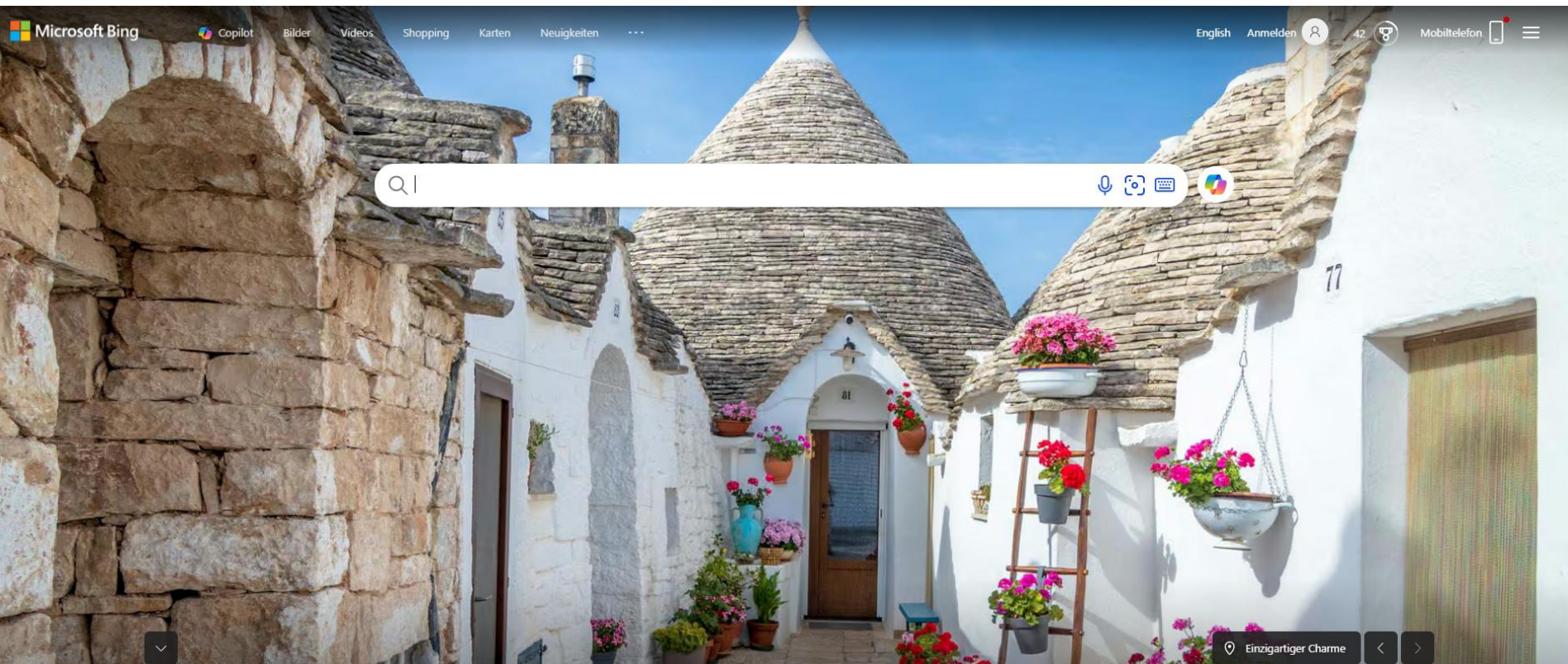
Rechtliche Grundlagen

Gesetzliche Rollen

- ▶ Verantwortlicher
- ▶ Auftragsverarbeiter
- ▶ Betroffene Person
- ▶ Rechtsgrundlage für die Offenlegung durch den Verantwortlichen
 - ▶ Reicht Art. 6 Abs. 1 lit. f DSGVO
 - ▶ Kompensiert § 25 Abs. 2 BDSG für öffentliche Stellen?


Ausgangslage & Problemstellung

War der PC mal wieder gesperrt und hatte einen schönen Hintergrund?
Schon ist man im Tracking von Bing gefangen.



Souverän in der IONOS Cloud und dann auf web.de?

IONOS LOGIN



Mein IONOS Login


Kundennummer, E-Mail-Adresse oder Domain


[Zugang vergessen?](#)

Weiter

Weitere IONOS Logins


Webmail


Data Center Designer


HiDrive

WEB.DE

Wir finanzieren uns über Werbung, um Ihnen Produkte kostenfrei anbieten zu können.

Postfach ohne Fremdwerbepartner abonnieren

Nutzen Sie WEB.DE mit Premium-Postfach ohne Fremdwerbepartner und ohne Werbetacking ab 3,99 €/Monat.*

Zum Abo ohne Fremdwerbung

Mit einem bestehenden MailPlus- oder Club-Vertrag können Sie die Option ohne Werbetacking [hier](#) kostenlos dazubuchen.

Option ohne Werbetacking bereits gebucht? [Hier anmelden](#).
Noch keinen WEB.DE Account? [Hier registrieren](#).

Mit Werbung und Tracking weiter wie gewohnt

Nutzen Sie WEB.DE wie gewohnt mit Werbetacking. Ihre Zustimmung ist jederzeit widerrufbar.

Akzeptieren und weiter

Mit einem bestehenden MailPlus- oder Club-Vertrag bleibt Ihr Postfach auch mit Zustimmung wie gewohnt ohne Fremdwerbepartner.


Details zu Werbe- und Analyse-Trackern sowie zum jederzeit möglichen Widerruf finden Sie in unserer [Datenschutzerklärung](#) oder im [Privacy Center](#).

Für die Nutzung mit Werbung und Tracking: Wir und unsere bis zu 267 Partner verarbeiten personenbezogene Daten wie beispielsweise Nutzerkennungen, um den Inhalt von WEB.DE zu optimieren und an Ihre Interessen anzupassen und fragen gegebenenfalls aktiv Ihre Geräteigenschaften zur Identifikation ab. Dafür und für die unten aufgeführten Verarbeitungszwecke benötigen wir und unsere Partner fortan Ihre Zustimmung. Diese umfasst auch Ihre Einwilligung in die Übermittlung bestimmter personenbezogener Daten in Drittländer nach Art. 49 Abs. 1 lit. a DSGVO. Solange die EU keinen Angemessenheitsbeschluss fasst, gilt grundsätzlich für die Übermittlung von Daten in Drittländer nicht das gleiche Sicherheitsniveau wie in der EU. Diese Übermittlung birgt daher Risiken, wie beispielsweise, dass die für die Übermittlung getroffenen technischen, organisatorischen und vertraglichen Maßnahmen nicht ausreichen, um zu verhindern, dass Ihre Daten von öffentlichen Stellen zu Kontroll- und Überwachungszwecken verarbeitet werden, möglicherweise auch ohne die Möglichkeit eines Rechtsbehalts. Unsere Partner können Sie hier einsehen.

Verarbeitungszwecke

Erst beim Server in AWS vorbei und dann Amazon?

Marktanteil von AWS in Deutschland?

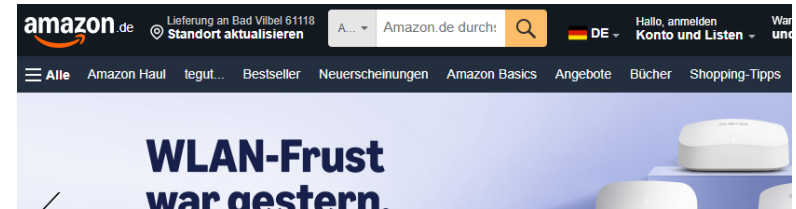
 Copilot ⓘ

Der Marktanteil von **Amazon Web Services (AWS)** in **Deutschland** liegt Schätzungen zufolge bei etwa **30–35 %** im Bereich der Public-Cloud-Infrastruktur ¹.
Damit ist AWS auch hierzulande der führende Anbieter, vor **Microsoft Azure** und **Google Cloud**.

Weitere Einblicke:

Übersicht deutscher Cloud-Initiativen bitte 

Nachricht an Copilot



Cookie- und Werbeeinstellungen

Wenn du zustimmst, können wir deine persönlichen Informationen von einem dieser [Amazon-Dienste](#) verwenden, um die Anzeigen, die wir dir auf anderen Diensten zeigen, zu personalisieren. Beispielsweise können wir deinen Prime Video-Wiedergabeverlauf verwenden, um die Werbung, die wir dir in unseren Stores oder auf Fire TV zeigen, zu personalisieren. Wir können auch persönliche Informationen verwenden, die wir von Drittanbietern erhalten (wie demografische Informationen).

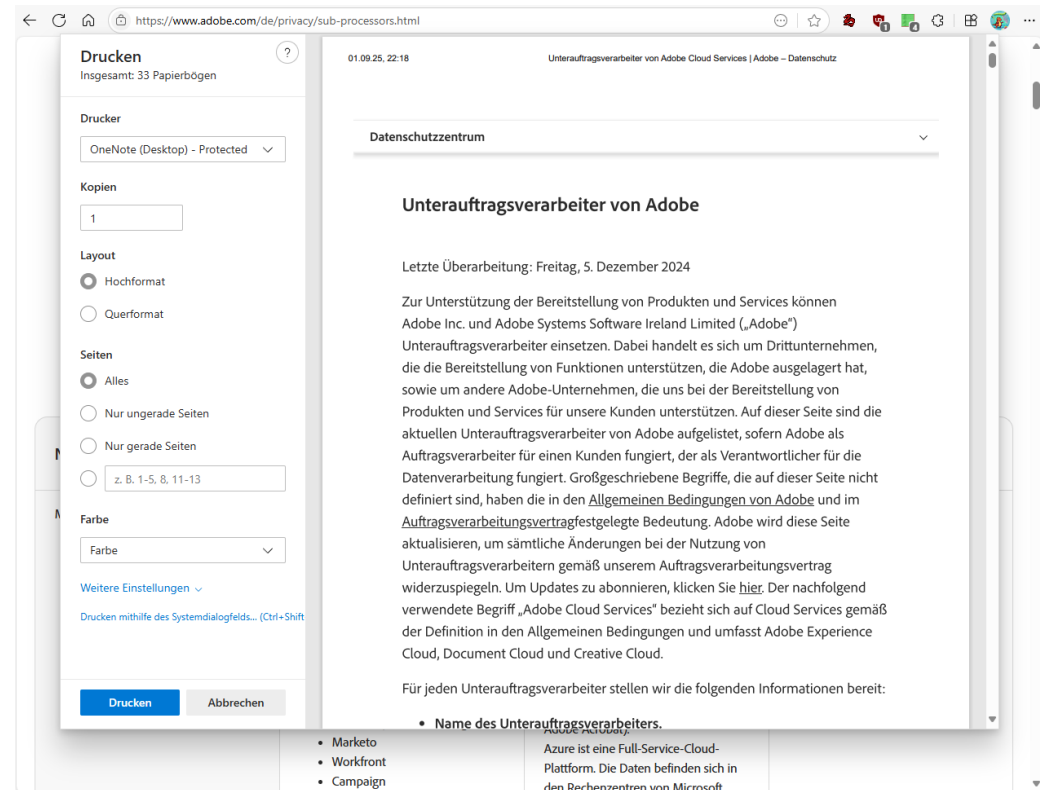
Wenn du zudem zustimmst, verwenden wir auch Cookies, um dein Einkaufserlebnis in den Amazon-Stores zu verbessern, wie in unserem [Cookie-Hinweis](#) beschrieben. Deine Wahl gilt für die Verwendung von Werbe-Cookies von Erstanbietern und Drittanbietern für diesen Service. Cookies speichern oder greifen auf Standardgeräteinformationen wie eine eindeutige Kennung zu. Die [101 Drittanbieter](#), die auf diesem Dienst Cookies verwenden, tun dies zu ihren Zwecken, um personalisierte Werbung anzuzeigen und zu messen, Einblicke in die Zielgruppe zu gewinnen und Produkte zu entwickeln und zu verbessern.

Wir verwenden jedenfalls Cookies und ähnliche Tools, die erforderlich sind, um dir das Tätigen von Einkäufen zu ermöglichen, dein Einkaufserlebnis zu verbessern und unsere Dienste bereitzustellen, wie in unserem [Cookie-Hinweis](#) beschrieben. Wir verwenden diese Cookies auch, um zu verstehen, wie Kunden unsere Dienste nutzen (z. B. durch Messung der Websiteaufrufe), damit wir Verbesserungen vornehmen können. Klicke auf „Ablehnen“, um abzulehnen, oder auf „Anpassen“, um detailliertere Werboptionen zu treffen oder mehr zu erfahren. Du kannst deine Auswahl jederzeit ändern, indem du [Cookie- und Werbeeinstellungen](#) besuchst. Um mehr darüber zu erfahren, wie und zu welchen Zwecken Amazon persönliche Informationen (wie den Bestellverlauf im Store oder den Prime Video-Wiedergabeverlauf) und Cookies verwendet, besuche bitte unsere [Datenschutzerklärung](#) und unseren [Cookie-Hinweis](#).

[Akzeptieren](#) [Ablehnen](#) [Anpassen](#)

Und was steht in den Verträgen?

- ▶ **AWS:** Begrenzung der Auftragsverarbeitung auf „Customer Data“
- ▶ **Microsoft:** Bing-Dienste nicht Teil des DPA
- ▶ **VERBI/MAXQDA:** Vertragsgeflechte mit Drittanbietern



Mögliche zulässige Mit- und Eigennutzungen

- ▶ Zweckänderung mit Offenlegung
 - ▶ Informationssicherheit
 - ▶ Updates
 - ▶ Kompatibilität
- ▶ Gesetzliche Pflichten als mittelbare Verarbeitungserlaubnis
 - ▶ U.a. NIS-RL, CRA, ...
- ▶ Leistung fällt unter ePrivacy-RL statt DSGVO (Telekommunikation)
- ▶ Data Act
 - ▶ Anwendbarkeit steht und fällt mit der Weite des Begriffs der personenbezogenen Daten
 - ▶ Mittelbar Legitimation für Profiling (OLG Köln (15. Zivilsenat), Urteil vom 23.05.2025 – 15 UKI 2/25 - GRUR-RS 2025, 10988)

Profilverkettung – Was ist das?

- ▶ **Profilverkettung** meint die Verknüpfung personenbezogener Daten aus verschiedenen Quellen oder Diensten – oft durch denselben Anbieter.
- ▶ Geht über klassisches **Profiling** (Art. 4 Nr. 4 DSGVO) hinaus.

Typische Szenarien:

- ▶ Auftragsverarbeiter nutzt Daten **nicht nur im Auftrag**, sondern auch **für eigene Zwecke**.
- ▶ Kombination von Daten aus der Auftragsverarbeitung mit **Nutzungsdaten anderer Dienste**.

Risiken für Betroffene und Auswirkungen

- ▶ Verknüpfung von Identitäten oder Onlinekennungen
- ▶ Intransparenz: Betroffene wissen nicht, wer ihre Daten verarbeitet und wofür.
- ▶ Rechtsverlust: Rechte auf Auskunft, Widerspruch und Löschung sind faktisch nicht durchsetzbar.
- ▶ Verantwortungsdiffusion: Anbieter verweisen auf „Anonymität“ oder den ursprünglichen Verantwortlichen – echte Verantwortlichkeit bleibt unklar.

Folgen für die Interessenabwägung (Art. 6 Abs. 1 lit. f DSGVO):

- ▶ Höheres Risiko → geringere Chance auf Rechtmäßigkeit der Verarbeitung
- ▶ Ohne Risikoreduktion (z. B. nur Auswertung aggregierter Daten, Pseudonymisierung, vereinfachte Widerspruchsmöglichkeiten) überwiegen die Interessen der Betroffenen

Lösungsansatz – Vertraglich

▶ Vertragliche Zusicherung

Beispiel „Microsoft 365 Copilot- und Microsoft 365 Copilot Chat

... Abfragedaten ...

- ▶ Microsoft hat keine Rechte an Abfragedaten über das zur Bereitstellung der Dienste erforderliche Ausmaß hinaus.
- ▶ Abfragedaten werden nicht zur Verbesserung von Bing verwendet.
- ▶ Abfragedaten werden nicht verwendet, um Werbepprofile zu erstellen oder das Nutzerverhalten nachzuverfolgen.
- ▶ Abfragedaten werden nicht an Werbetreibende oder anderweitig über Microsoft und seine Vertragslieferanten hinaus weitergegeben, die Bestimmungen unterliegen, die nicht weniger Schutz bieten als diese Bestimmungen.
- ▶ Abfragedaten werden nicht zum Trainieren von Grundlagenmodellen für generative KI verwendet.
- ▶ Abfragedaten werden als vertrauliche Kundeninformationen behandelt und durch entsprechende technische und organisatorische Maßnahmen geschützt.

<https://www.microsoft.com/licensing/terms/productoffering/Microsoft365/MCA>

Technisch-organisatorische Maßnahmen

- ▶ Gehärteter Unternehmensbrowser
- ▶ Anbieter-Diversifizierung
- ▶ Proxy-Dienste für den Zugriff
- ▶ Nutzeraufklärung



UNIVERSITÄTSBIBLIOTHEK

🏠 > UNIVERSITÄTSBIBLIOTHEK > SUCHEN & AUSLEIHEN > ELEKTRONISCHE MEDIEN NUTZEN
> DATA-TRACKING

Schutz vor Data-Tracking durch Wissenschaftsverlage

Einige Verlage und Anbieter verfolgen das Rechercheverhalten der Nutzerinnen und Nutzer, erstellen Profile und werten diese Informationen ohne Zustimmung der Betroffenen für eigene Zwecke aus (Data-Tracking).

▶ Wie wir Sie vor Data Tracking schützen.

▶ Wie Sie sich vor Data Tracking schützen können.

Kontakt

Information
Tel.: +49 931 31-85906
E-Mail: ub-information@uni-wuerzburg.de

Audit eines Auftragsverarbeiters

- ▶ **Untersuchung durch:** Niederländisches Ministerium für Justiz & Sicherheit + EY (März 2021)
- ▶ **Ziel:** Bewertung der Risiken unerlaubten Profilings bei Microsoft 365
- ▶ **Ergebnis:**
 - *Geringes Risiko* für unerlaubtes Profiling
 - Fokus auf Schutzmechanismen statt auf Nachweis einzelner Verstöße
 - Motto: „*Prevent a needle to exist – and detect it if it does*“
- ▶ **Methodik:**
- ▶ Strukturierung entlang des **Lebenszyklus personenbezogener Daten**
- ▶ Systematisierte Datenschutz- und Profiling-Kontrollen im Prüfbereich
- ▶ **Praxisrelevanz:**
- ▶ **Design & Wirksamkeit** der Kontrollmechanismen entscheidend
- ▶ Auch bei potenziellen Verstößen: **wirksame Abgeltung durch Kontrollen**

Fazit

- ▶ Auftragsverarbeitung auf mit Eigeninteressen
- ▶ Gefahr von Erkenntnisverknüpfungen über betroffene Personen deren Daten im Kontext der Auftragsverarbeitung und gleichzeitig auch in einem weiteren Angebot des „Auftragsverarbeiters“ anfallen
- ▶ Prüfstein für das „Freiwilligkeitserfordernis“ in Art. 7 DSGVO?
- ▶ Transparenz, Kontrolle und Gestaltung sind entscheidend
- ▶ Verantwortliche können in Grenzen Schutz schaffen für betroffene Personen
- ▶ Lösungsmöglichkeiten durch den Gesetzgeber
 - ▶ Jährliche proaktive Datenschutzauskunft
 - ▶ Ausweitung oder Einführung von Zusammenführungsverbote
 - ▶ gesetzliche gemeinsame Verantwortlichkeit, wenn Auftragsverarbeiter Daten aus dem Zusammenhang der Auftragsverarbeitung auch für eigene Zwecke verarbeitet

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

it-recht@digitalverbund.bayern

Soziale Netzwerke

Johannes Nehlsen mit dem Handle @JoNehlsen